

HP OpenView

Storage Mirroring application notes

High availability for Clustered Exchange servers

Legal and notice information

© Copyright 2005 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, Windows NT®, Windows XP®, and Windows Server™ are U.S. registered trademarks of Microsoft Corporation.

Storage Mirroring High availability for Clustered Exchange servers application notes

Introduction

Microsoft Exchange Server is a messaging and collaboration server for the most demanding business needs. Its scalability, performance, and enhanced security make Exchange an ideal messaging foundation for enterprise networks. Storage Mirroring provides real-time enterprise data protection and replication for cluster environments. Storage Mirroring can be used to provide high availability for your Exchange server.

This document describes the steps necessary to configure Storage Mirroring to provide high availability and disaster recovery for two clusters running Windows 200x, Cluster Service, and Microsoft Exchange Server version 2000 or 2003.

In addition to the Exchange Information Stores (mailboxes and public folders), there are many important aspects of an Exchange server configuration that are required for Exchange functionality following the loss of a production Exchange Server. It is important to be aware of the overall production Exchange server configuration and to configure the target server identically. Some configuration aspects fall outside the scope of this document such as the configuration of any Exchange Connectors, Built-In Instant Messaging, Newsgroups, Bridgehead Servers, and so on. These issues need to be addressed exclusively by the Exchange administrator.

To complete these instructions, you will install Microsoft Exchange Server and Storage Mirroring, then configure Storage Mirroring for replication and failover. Due to the complexities of these applications, this document is intended for network administrators with experience installing, configuring, and maintaining network applications, including Storage Mirroring, Cluster Service, and Microsoft Exchange Server.

Requirements

Each node in each cluster must meet the following system requirements.

- One of the following operating systems:
 - Microsoft Windows 2000 Advanced Server with Service Pack 3 or later
 - Microsoft Windows Server 2003 Enterprise Edition



NOTE: All nodes must be running the same operating system.

- One of the following Microsoft Exchange Server versions:
 - Microsoft Exchange Server 2000 Enterprise Edition with Service Pack 3 or higher
 - Microsoft Exchange Server 2003 Enterprise Edition



NOTE: HP recommends that the Exchange version be the same as the operating system version.

- A licensed copy of Storage Mirroring version 4.3.4 or later
- A copy of the Exchange Failover utility (`exchfailover.exe`) version 2.1.
- Each node must be a member server in the same domain

Backing up your environment

Before beginning these procedures, make sure you have a current backup of all nodes. Also, make sure you have a complete backup of Active Directory.

Environment verification

Before you use the Exchange Failover utility, complete the following tasks to verify that the environment is properly set up.

1. With both Exchange servers online, use Active Directory Users and Computers to move an existing user from the source to the target and then back to the original source.
2. Verify that you can create a new user on the target.
3. To verify connectivity, create an Outlook profile for the new user on a client machine and connect to the target.

Configuring the source cluster

For the source cluster, you will need to complete the following:

- ["Installing Exchange"](#) on page 4
- ["Creating the source cluster Exchange virtual server"](#) on page 5
- ["Installing Storage Mirroring on the source cluster"](#) on page 12
- ["Configuring Storage Mirroring on the source cluster"](#) on page 12
- ["Creating the replication sets"](#) on page 12

If Exchange is already installed on your source cluster, you can skip to section ["Configuring Storage Mirroring on the source cluster"](#) on page 12. However, you must make sure you know the configuration information (storage groups, databases, paths, and file names) so that the target cluster can be configured identically.

If Storage Mirroring is already installed, review ["Configuring Storage Mirroring on the source cluster"](#) on page 12 to make sure your configuration matches the required configuration for this Exchange solution.

Installing Exchange

Download the Microsoft document that is appropriate for your Exchange version and service pack level to prepare the forest and domain and install Exchange on each node of the source cluster. These documents can be found on the Microsoft web site. Apply any Exchange service packs or patches. Record critical Exchange configuration information from the source cluster, including storage groups, databases, paths, and file names so that this information can be used when installing Exchange on the target.

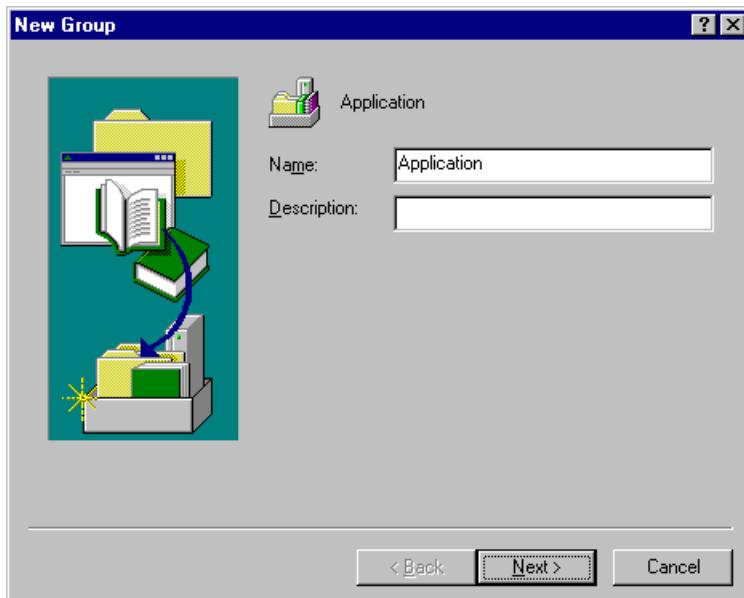
Creating the source cluster Exchange virtual server

To create the Exchange virtual server, you will be creating an Exchange group and adding the following resources:

- IP address
- Network name
- Physical Disk Resource
- Exchange System Attendant

Creating the Exchange group

1. Right-click the **Groups** folder on the left pane of the Cluster Administrator and select **New, Group**. The New Group dialog box will appear.



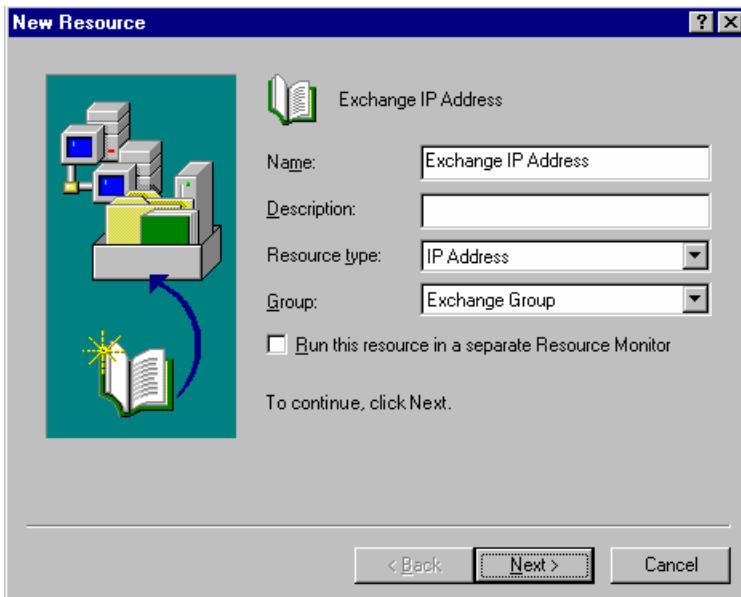
2. Specify the **Name** (such as "Exchange Group") and **Description** for the Exchange group and click **Next** to continue.
3. **No Preferred Owners** are required. Click **Finish** to complete the creation of the new group.



NOTE: You will be notified that the group was created successfully. Click **OK** to acknowledge the message and return to the Cluster Administrator main screen.

Creating the Exchange IP Address resource

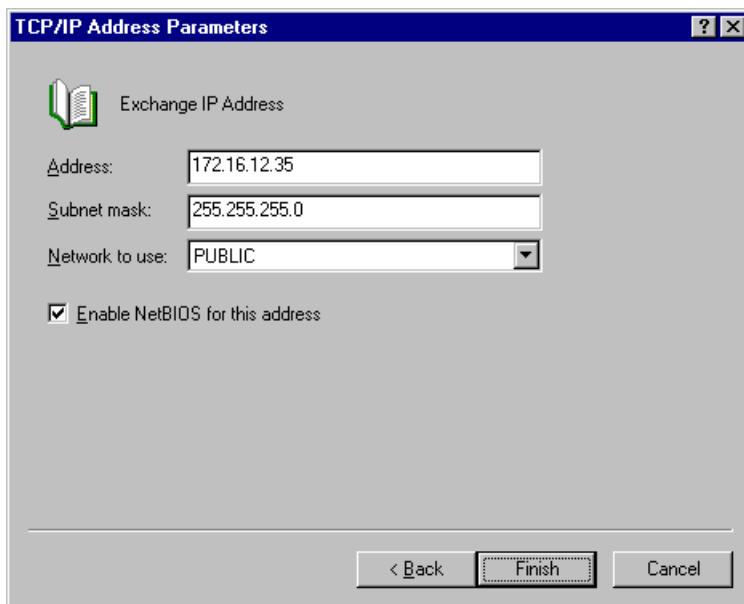
1. Right-click the Exchange group that you just created and select **New, Resource**. The New Resource dialog box will appear.
2. Specify the following fields on the New Resource dialog box:



- **Name**—Specify a name that identifies this resource as the IP address for the Exchange group (such as "Exchange IP Address"). This name must be unique within the cluster.
- **Description**—You can optionally add a more detailed description for this resource.
- **Resource type**—Specify **IP Address**.
- **Group**—The Exchange group you created in "[Creating the Exchange group](#)" should be selected. If it is not, select the correct group name.

3. Click **Next** to continue.
4. The default **Possible Owners** does not need to be modified. Click **Next** to continue.
5. There are no **Dependencies** required. Click **Next** to continue. The TCP/IP Address Parameters dialog box will appear.

6. Specify the following fields on the TCP/IP Address Parameters dialog box:



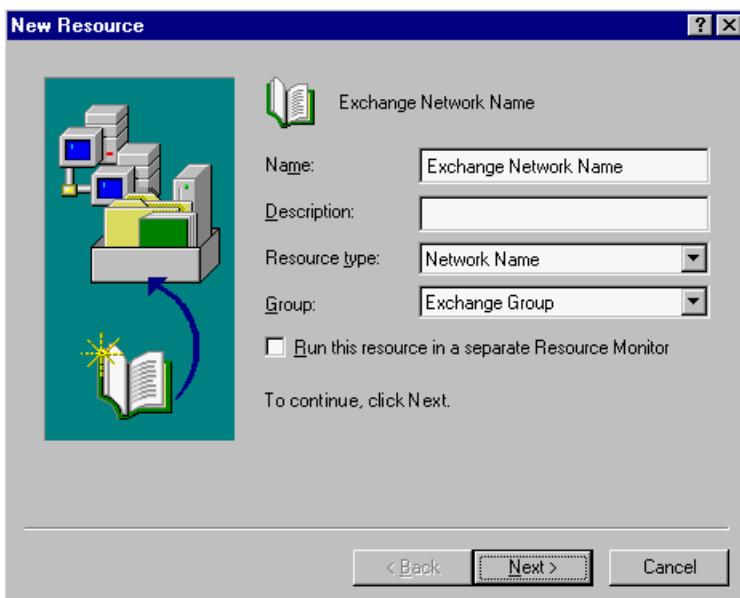
- **Address**—Enter the IP address that will be assigned to the Exchange virtual server.
- **Subnet mask**—Enter the subnet mask associated with the IP address you just entered.
- **Network to use**—If you have more than one route for network traffic defined, specify the network that this IP address will use.

7. Click **Finish** to complete the creation of the IP address resource.

8. Right-click the IP address resource and select **Bring Online**.

Creating the Exchange network name resource

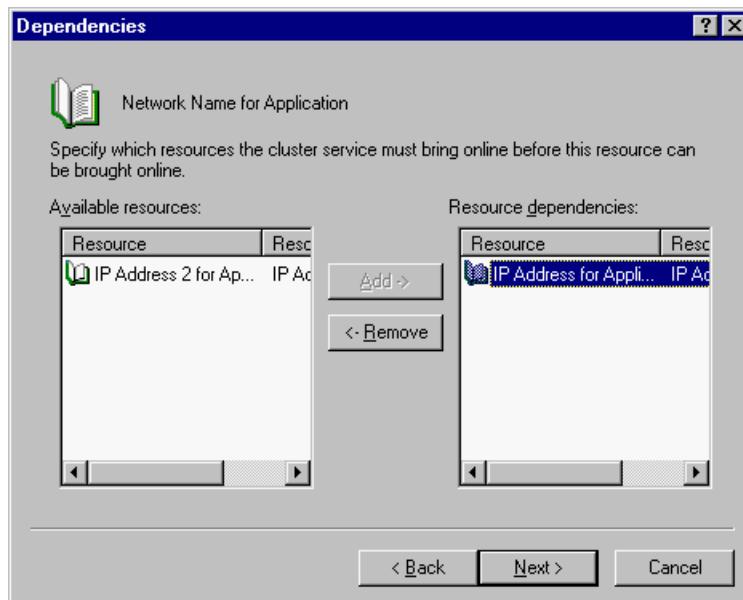
1. Right-click the Exchange group and select **New, Resource**. The New Resource dialog box will appear.
2. Specify the following fields on the New Resource dialog box:



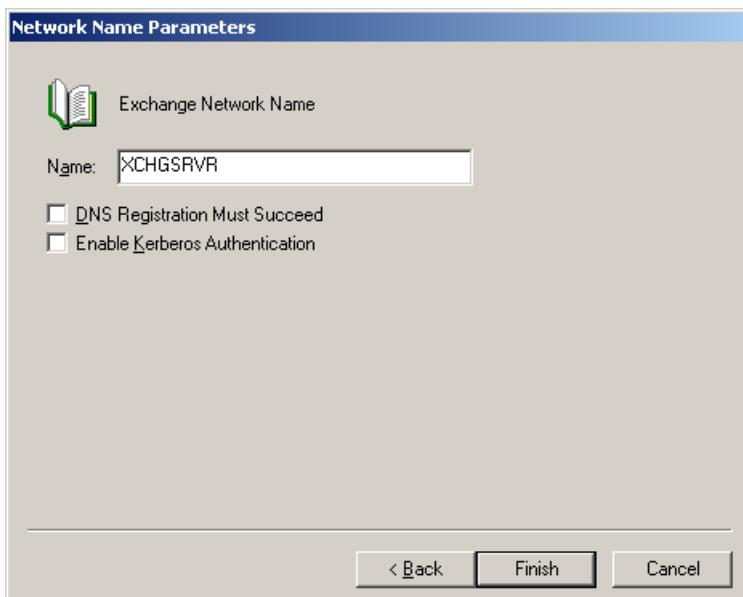
- **Name**—Specify a name that identifies this resource as the virtual server name for the Exchange group (such as "Exchange Network Name"). This name must be unique within the cluster.
- **Description**—You can optionally add a more detailed description for this resource.
- **Resource type**—Specify **Network Name**.
- **Group**—The Exchange group you created in "[Creating the Exchange group](#)" should be selected. If it is not, select the correct group name.

3. Click **Next** to continue.
4. The default **Possible Owners** does not need to be modified. Click **Next** to continue. The Dependencies dialog box will appear.

5. An IP address must be present in order for a Network Name to be assigned. Therefore, move the IP address resource that you created in “[Creating the Exchange IP Address resource](#)” to the **Resource dependencies** list.



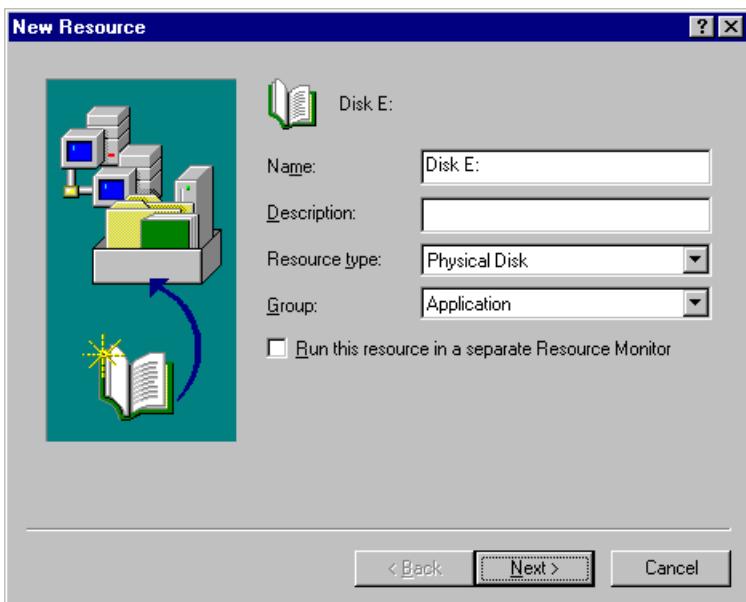
6. Click **Next** to continue. The Network Name Parameters dialog box will appear.
7. Specify the Network Name Parameters by entering the virtual name of the Exchange server. This is the name that clients will look for on the network.



8. Click **Finish** to complete the creation of the Exchange virtual server Network Name resource.
9. Right-click the Network Name resource and select **Bring Online**.

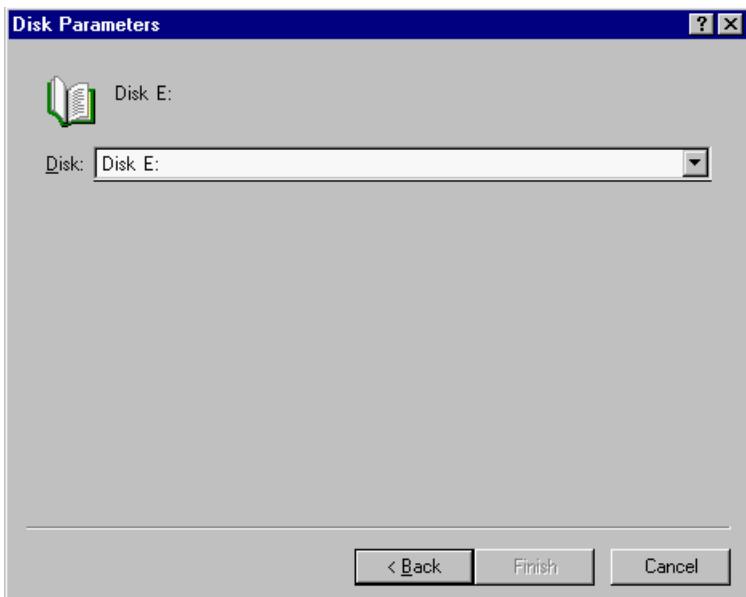
Creating the physical disk resource

1. Right-click the group and select **New, Resource**. The New Resource dialog box will appear.
2. Specify the following fields on the New Resource dialog box:



- **Name**—Specify a name that identifies the disk drive associated with the virtual server (such as "Disk E:"). This name must be unique within the cluster.
- **Description**—You can optionally add a more detailed description for this resource.
- **Resource type**—Specify **Physical Disk**.
- **Group**—The Application group name should be selected. If it is not, select the correct group name.

3. Click **Next** to continue.
4. Verify that both nodes appear as **Possible Owners** and click **Next** to continue.
5. No resources are required as dependencies. Click **Next** to continue. The Disk Parameters dialog box will appear.
6. Specify the disk drive associated with the physical disk resource.



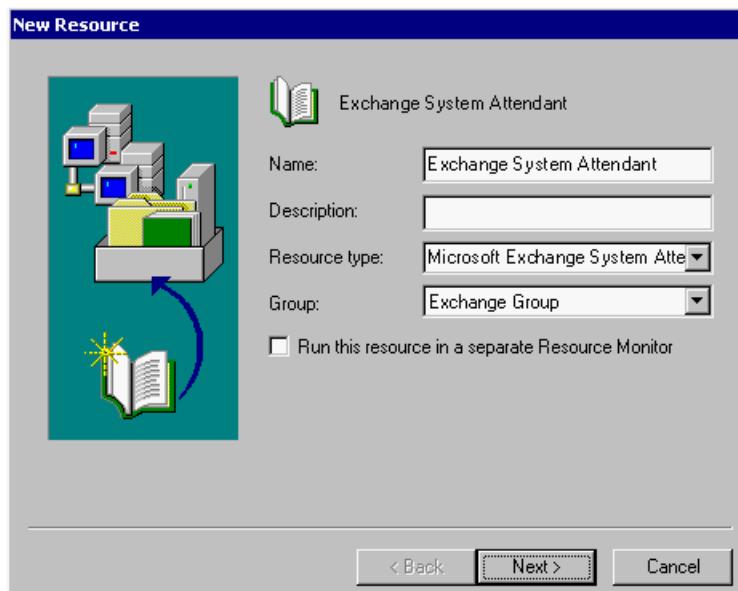
7. Click **Finish** to complete the creation of the Physical Disk resource.
8. Right-click the physical disk resource and select **Bring Online**.
9. Some Exchange implementations separate the databases and log files on to different disk resources for improved disk I/O. If this is the case in your environment, repeat steps 1-8 and create additional physical disk resources for each disk.

Creating the Exchange system attendant resource



NOTE: Using Exchange System Manager, verify that the Cluster Service account is an Exchange Full Admin.

1. In the Cluster Administrator, right-click the Exchange group and select **New, Resource**. The New Resource dialog box will appear.
2. Specify the following fields on the New Resource dialog box:



- **Name**—Specify a name that identifies the Exchange System Attendant (such as "Exchange System Attendant").
- **Description**—You can optionally add a more detailed description for this resource.
- **Resource type**—Specify **Microsoft Exchange System Attendant**.
- **Group**—The Exchange Group should be selected. If it is not, select the correct group name.

3. Click **Next** to continue.
4. Verify that both nodes are listed as possible owners. Click **Next**.
5. The Exchange System Attendant resource is dependent on the Exchange virtual server Network Name and the physical disk resource. Move the Exchange Server Name and the physical disk resource that you just created to the **Resource dependencies** list and click **Add** to continue.
6. Verify the administrative groups are correct. Click **Next**.
7. Verify that the routing groups are correct. Click **Next**.
8. Verify the location of the Exchange data files, for example `E:\Exchsrvr`. Click **Finish**.
9. Right-click the Exchange resource group. Select **Bring Online**.

Installing Storage Mirroring on the source cluster

1. Install Storage Mirroring on each node of the source cluster, if it is not already installed. See the *HP OpenView Storage Mirroring getting started guide* for installation instructions.
2. Run the `setup.exe` file to install the Exchange Failover Utility in the Storage Mirroring directory on each node where Storage Mirroring is installed.

Configuring Storage Mirroring on the source cluster

1. Start the Storage Mirroring Management Console by selecting **Start, Programs, Storage Mirroring, Management Console**.
2. Double-click on the first node on the left pane of the Management Console to login.
3. Right-click the first node of the cluster and select **Properties**.
4. Select the **Setup** tab.
5. By default, the **Automatically Reconnect During Source Initialization** check box will be selected. Disable this option by clearing the check box.
6. In the **Properties** dialog box, select the **Source** tab.
7. By default, the **Block Checksum All Files on a Difference Mirror** check box will not be selected. Enable this option by marking the check box.
8. Click **OK** to save the changes.
9. Repeat steps 2 - 8 on the second node of the cluster.

Creating the replication sets

In order for the clusters to be synchronized, the data that is changed on the source cluster must be replicated to the target cluster. Storage Mirroring handles this task by establishing identical replication sets on each node of the source cluster that identify the data that is changing. Only the replication set of the node that owns the Exchange resource group will be online at any given time, ensuring that only the changing data from the owning node is replicated.

Creating the Storage Mirroring replication set on the owning node

1. In the left pane of the Storage Mirroring Management Console, right-click the node that owns the Exchange group that you wish to protect and select **New, Replication Set**.
2. Enter a name for the replication set and press **Enter**.
3. Select the drive(s) that contain the Exchange database and log files. The MDBDATA, MAILROOT, and MTADATA directories must be included.
4. Right-click the replication set name and select **Save**.
5. Right-click the replication set that you just created and select **Properties**.
6. Record the exact drive and directories of each path displayed in the Replication Set Properties table below. Place a check mark or X in the Include, Exclude, and Recurse Sub-directories columns to identify which parameters apply to the specified path.

Replication Set Properties

Drive and Directories	Include	Exclude	Recurse Sub-directories

Creating the Storage Mirroring replication set on the non-owning node

1. Double-click on the second node on the left pane of the Management Console to login.
2. Right-click the node and select **New, Replication Set**.
3. Enter the exact, case-sensitive name for the replication set as specified on the first node and press **Enter**.
4. Right-click the replication set that you just created and select **Properties**.
5. Click **Add**.
6. Enter one of the drive and directory paths that you recorded in the table "[Replication Set Properties](#)". Be sure to mark the correct Include, Exclude, and Recurse sub-directories options that need to be applied.



NOTE: Each replication set rule *must* be identical to the replication set rule on the first node in order for the disaster recovery process to work correctly.

7. Click **OK** to save the replication set rule.

8. Repeat steps 5–7 for each path and directory on the first node.



NOTE: Each drive and directory will appear in the Replication Set Properties even though the second node may not have access to these locations right now. That is not a problem.

9. Right-click the replication set name and select **Save**.



NOTE: You will be completing the rest of the source cluster configuration after the target cluster has been configured.

Configuring the target cluster

For the target cluster, you will need to complete the following:

- “[Installing Exchange on the target cluster](#)” on page 14
- “[Creating the target cluster Exchange virtual server](#)” on page 14
- “[Verifying the Exchange log file prefixes](#)” on page 14
- “[Installing Storage Mirroring on the target cluster](#)” on page 15
- “[Configuring Storage Mirroring on the target cluster](#)” on page 15

This target Exchange virtual server will be kept offline until a failure occurs.

Installing Exchange on the target cluster

Install Exchange on the target cluster with the same configuration as the source cluster, matching storage groups, databases, paths, and file names.

Creating the target cluster Exchange virtual server

Repeat the steps in “[Creating the source cluster Exchange virtual server](#)” on page 5 to create another Exchange virtual server on the target cluster and bring it online. The Exchange virtual server Network Name and the Exchange IP address resources in this group *must* be unique from those on the source cluster; however, the physical Exchange database and log file drive/directory structure must be identical to the source cluster’s Exchange database and log file drive/directory structure.

Verifying the Exchange log file prefixes

When you installed Exchange on the source, the default Exchange storage group was assigned E00 as the prefix of the log files. The second storage group was assigned E01, the third E02, and so on. The storage groups on the target must have the same numbering scheme. If you have one or two storage groups on your source, you can continue with the next section. If you have more than two storage groups on your source, verify that the prefix numbering is the same on the source and target virtual Exchange servers.

1. Using the Exchange System Manager on the source, select the source Exchange server. Right-click each storage group and select **Properties**. Record the prefix number assigned to each storage group.
2. On the target, use the Exchange System Manager to check the prefix number assigned to each storage group.

3. If the storage group prefix numbers are identical, you can continue with the next section. If the storage group prefix numbers are different, you will need to modify them. You can do this by deleting the storage groups and re-creating them in the same order they were created on the source, or you can use ADSIEDit to modify the prefix numbers. Using ADSIEDit, modify the properties of the entry noted below to change the msExchESEParamBaseName on the Properties page to match that of the source. The entry that must be edited is

```
CN=First_Storage_Group_Name, CN=Information Store,  
CN=Exchange_Server_Name, CN=Servers, CN=First_Administrative_Group_Name,  
CN=Administrative Groups, CN=Exchange_Organizational_Name, CN=Microsoft  
Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com
```

You will have to use ADSIEDit from the Windows Support Tools to make this change. See your Windows reference guide for more information.

Installing Storage Mirroring on the target cluster

1. Install Storage Mirroring on each node of the target cluster. See the *HP OpenView Storage Mirroring getting started* guide for installation instructions.
2. Install the Exchange Failover utility. Run the `setup.exe` file downloaded from the web site to install the Exchange Failover utility on each node where Storage Mirroring is installed.

Configuring Storage Mirroring on the target cluster

1. Start the Storage Mirroring Management Console by selecting **Start, Programs, Storage Mirroring, Management Console**.
2. Double-click on the first node of the target cluster in the left pane of the Management Console to login.
3. Right-click the first node of the target cluster and select **Properties**.
4. Select the **Setup** tab.
5. By default, the **Automatically Reconnect During Source Initialization** check box will be selected. Disable this option by clearing the check box.
6. In the **Properties** dialog box, select the **Source** tab.
7. By default, the **Block Checksum All Files on a Difference Mirror** check box will not be selected. Enable this option by marking the check box.
8. Click **OK** to save the changes.
9. Repeat steps 2–8 on the second node of the target cluster.

Taking the resources offline

On the target cluster, take the Exchange virtual server Network Name resource offline.

The rest of the Exchange resources should come offline automatically since they are dependent upon the Exchange virtual server Network Name resource, leaving only the Exchange virtual server IP address(es) and the disk resources online.

Completing the source configuration

To complete the source configuration, you need to complete the following:

- “Configuring the Storage Mirroring source connection resource on the source cluster” on page 16
- “Editing the online scripts” on page 16
- “Bringing the components online” on page 17

Configuring the Storage Mirroring source connection resource on the source cluster

The Storage Mirroring Source Connection resource controls the Storage Mirroring connections. You need to configure this resource on the source cluster through the Cluster Administrator.

1. Select **Start, Programs, Administrative Tools, Cluster Administrator**.
2. Right-click on the Exchange resource group and select **New, Resource**. The New Resource dialog box will appear.
3. Specify the following fields on the New Resource dialog box:
 - **Name**—Specify a name that indicates this is the Storage Mirroring virtual server connection (such as "Storage Mirroring Virtual Server Connection").
 - **Description**—You can optionally add a more detailed description for this resource.
 - **Resource type**—Specify **Storage Mirroring Source Connection**.
 - **Group**—The Application group name should be selected. If it is not, select the correct group name.
4. Click **Next** to continue.
5. Verify that both nodes appear as **Possible Owners** and click **Next** to continue.
6. To keep the Storage Mirroring Source Connection resource from coming online before the physical disk, make this resource dependent on all physical disk resources within the source Exchange group. Click **Next** to continue.
7. Specify the following on the Storage Mirroring Source Connection Parameters dialog box:
 - **Replication Set**—Specify the name of the Storage Mirroring replication set. This name is case-sensitive and should be the same name as specified in "[Creating the replication sets](#)" on page 12.
 - **Storage Mirroring Target**—Specify the unique Exchange virtual server IP address that is online on the target cluster.The other options on the Storage Mirroring Source Connection Parameters dialog box are optional. See the *HP OpenView Storage Mirroring user's guide* for more information.
8. Click **Finish** to complete the creation of the Storage Mirroring Source Connection resource.

Editing the online scripts

You will need to modify one of the scripts which control the Storage Mirroring Source Connection resource to enable orphan file removal.

1. Open the file `online.dtcl`, located in the directory where you installed Storage Mirroring, with a text editor.
2. Locate the following section in the file.

```
if ($exitcode = 0) then
    WRITE "Starting block checksum mirror";
    $mirror = MIRROR START $conid DIFFERENT,CHECKSUM;
```

3. Add a space and the keyword `ORPHANS` (before the semicolon) to the last line in this section so that it is identical to the following command:
`$mirror = MIRROR START $conid DIFFERENT,CHECKSUM ORPHANS;`
4. Save and close the file.

5. Repeat steps 1–4 on the second node of the cluster.



NOTE: If Storage Mirroring auto-disconnects any connections, for example, because the queue space has been exhausted, Storage Mirroring will reconnect these connections as soon as it is possible. However, these subsequent connections will not have orphan file removal enabled. If you experience an auto-disconnect, you must manually run orphan file removal. In the Storage Mirroring Management Console, right-click an established connection and select **Remove Orphans, Start**. See the *HP OpenView Storage Mirroring user's guide* for information on remirror and restore procedures.

Bringing the components online

Bring the components online. Right-click the source cluster Exchange group and select **Bring Online**. Verify that all of the resources in the group are brought online successfully.

Storage Mirroring will now mirror all of the current Exchange data to the target cluster as well as begin replicating changes to the Exchange data.



NOTE: If you start Exchange Server and mount the replicated databases on the target, or if the data on the target is otherwise modified, the data on the source and target will no longer match. If the updated data on the target is not needed, perform a full or difference with block checksum mirror from the source to the target. If the updated data on the target is needed, restore the data from the target to the source. See the *HP OpenView Storage Mirroring user's guide* for information on remirror and restore procedures.

Dealing with a failure



NOTE: If your target cluster is on a different subnet from the source cluster, see "Appendix 2: WAN failover" on page 24.

In the event that the entire source cluster fails, you will need to perform some or all of the following steps before the clients can reconnect to the target cluster.

1. In a command prompt window, change to the Storage Mirroring directory, then execute the following command:

```
exchfailover -setup -failover -s source_Exchange_virtual_name  
-t target_Exchange_virtual_name
```

where *source_Exchange_virtual_name* is the name of the source Exchange virtual server and *target_Exchange_virtual_name* is the name of the target Exchange virtual server.

2. In order for the target cluster virtual Exchange server to stand in for the source, the target virtual Exchange server must have duplicates of the source virtual Exchange server's IP address.
 - a. Right-click within the target cluster Exchange resource group and choose **New, Resource**.
 - b. Create an IP address resource that is identical to the IP address resource of the source Exchange virtual server. No dependencies are required for an IP address resource.
3. Add the duplicate source virtual IP address to the target Exchange Network Names dependency list.
4. Bring the Exchange group on the target cluster online.

5. If your source had the routing master, you will need to modify the security settings so that the routing master role will be updated. You have two options available for modifying the security settings for the routing master role:
 - The first option grants the Exchange Failover utility the permission to perform the task for you. If you want to use this option, add the `-u username:password` switch as outlined in "[Exchange Failover Utility command syntax](#)" on page 33 to the `exchfailover` command in the following step. Specify the Exchange administrator account information.
 - The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and fallback scripts. You will have to use ADSIEDit from the Windows Support Tools to make this change. See your Windows reference guide for more information.
 - a. Open ADSIEDit and go to `CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.
 - b. Right-click on the entry. Choose **Properties**.
 - c. Select the Security tab. Click **Advanced**.
 - d. Click **Add**. Click on **Object Types**.
 - e. Verify that **Computers** are selected. Click **OK**.
 - f. Type in your `target_name` and click **CheckName**.
 - g. Select **Full Control**. Click **OK**.
6. You will need to run the Exchange failover utility again to prepare the databases for use. In a command prompt window, execute the following command:

```
exchfailover -failover -s source_Exchange_virtual_name  
-t target_Exchange_virtual_name
```

where `source_Exchange_virtual_name` is the name of the source Exchange virtual server and `target_Exchange_virtual_name` is the name of the target Exchange virtual server.



NOTE: You can automate steps 1, 4, and 6 by using the commands below. Step 5 can only be automated if you select the first option for modifying the security settings. The commands are case-sensitive and you will need to substitute the name of your source virtual server, target virtual server, and the Exchange group.

```
exchfailover.exe -setup -failover -s source_Exchange_virtual_name -t  
target_Exchange_virtual_name  
cluster /cluster:"target_cluster_name" group "target_Exchange_Group_Name" /ONLINE  
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 25000  
exchfailover.exe -failover -s source_Exchange_virtual_name -t  
target_Exchange_virtual_name
```

Configuring the HTTP protocol for Outlook web access

In order for Outlook Web Access clients to locate the user mailboxes, the following steps need to be performed on the target.

1. From the Exchange System Manager on the target, select **Administrative Groups**, **First Administrative Group**, **Servers**, the name of the target virtual server, **Protocols**, and **HTTP**.
2. Right-click on the Exchange virtual server in the right pane of the Exchange System Manager and select **Properties**.
3. On the General tab, click **Advanced**.
4. Click **Add**.
5. Select the IP address of the source Exchange virtual server. Click **OK** to return to the Advanced dialog box.
6. Click **OK** to return to the Properties dialog box.
7. Click **OK** again to close the Properties dialog box.

Once the commands are completed, clients can connect through Outlook Web Access to receive their e-mail.



NOTE: After failover, you may need to use the Active Directory Sites and Services applet to force domain controller replication before clients can connect. You may also need to manually close and reopen Outlook 2000 clients.

Failing back to your source cluster

To fail back to your source cluster, you will need to complete the following:

- “[Updating the source with the new data from the target](#)” on page 19
- “[Taking the resources offline](#)” on page 20
- “[Bringing the source Exchange group online](#)” on page 20

Updating the source with the new data from the target

During the source downtime, users are updating data on the target cluster. When your source cluster is ready to come back online, the data is no longer current and must be updated with the new data on the target cluster.

1. Bring one or both of the source cluster nodes online, but do not allow the Exchange group to start.



NOTE: Log on locally, and if necessary, disconnect one cluster node from the production network and bring it online. Take any Exchange resources offline, reconnect the node to the network, log off, then log into the domain.

You may need to start the cluster from a command line. From a command prompt, type CLUSTER /? for help.

2. Using the instructions in “[Creating the replication sets](#)” on page 12, create a replication set on the target cluster that includes all of the volumes contained in the target Exchange resource group.
3. Bring the physical disk resource on the source cluster online.

4. Using the instructions in "Completing the source configuration" on page 15, create the Storage Mirroring Source Connection resource to the source cluster node IP address (not the source cluster virtual Exchange server IP address, which is offline). Modify the script and bring the resource online so that mirroring and replication to the source cluster can begin.
5. Monitor the mirroring process to ensure that it completes with no errors. The mirroring process is complete when the **Mirror Status** is **Idle**. Users may continue to access Exchange on the target cluster server.

After the mirror completes, schedule downtime to convert operations back to the source cluster.

Taking the resources offline

At the scheduled downtime, you will be taking the Exchange resources offline, removing an Exchange dependency, and deleting two resources.

1. Remove the source virtual IP address from the HTTP properties. This is what you configured in "Configuring the HTTP protocol for Outlook web access" on page 19.
2. Take the target Exchange IP and duplicate source IP offline. This should take every resource in the group offline except for the Storage Mirroring Source Connection and the disk resource(s).



NOTE: Clients will be unable to access Outlook at this time.

3. Verify that all of the data in queue on the target cluster has been applied to the original target before continuing. You can verify that the target queue is empty by checking the Bytes in Target Disk Queue statistic in the Target section of DTStat or the Bytes in Queue statistic in the Storage Mirroring Target section of Performance Monitor. If these statistics are zero (0), the queue is empty and you can continue. If these statistic are not zero, there is still data in queue on the target and you must wait before continuing. (For information on DTStat and Performance Monitor statistics, see the *HP OpenView Storage Mirroring user's guide*.)
4. Once all of the data has been replicated, take the Storage Mirroring Source Connection resource offline on the target and then delete it.



NOTE: The Storage Mirroring Source Connection resource on the target is no longer needed after data has been restored to the original cluster.

5. Remove the duplicate source IP from the target Exchange Network Name dependency list. Delete the duplicate source IP.

Bringing the source Exchange group online

Complete the following steps to bring the source Exchange group online.

1. In a command prompt window, change to the Storage Mirroring directory, then execute the following commands:

```
exchfailover -setup -failback -s source_Exchange_virtual_name  
-t target_Exchange_virtual_name
```

```
exchfailover -failback -nopublicfolders -s source_Exchange_virtual_name  
-t target_Exchange_virtual_name
```

where *source_Exchange_virtual_name* is the name of the source Exchange virtual server and *target_Exchange_virtual_name* is the name of the target Exchange virtual server.

2. Bring the target Exchange virtual IP address online so that the Storage Mirroring Source Connection can connect.

3. If you moved the routing master role to the target, you will need to modify the security settings so that the routing master role will be updated back to the source. You have two options available for modifying the security settings for the routing master role:

- The first option grants the Exchange Failover utility the permission to perform the task for you. If you want to use this option, add the `-u username:password` switch as outlined in the table “[Exchange Failover Utility command syntax](#)” on page 33 to the `exchfailover` command in the following step. Specify the Exchange administrator account information.
- The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and fallback scripts. You will have to use ADSIEDit from the Windows Support Tools to make this change. See your Windows reference guide for more information.
 - a. Open ADSIEDit and go to `CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.
 - b. Right-click on the entry. Choose **Properties**.
 - c. Select the Security tab. Click **Advanced**.
 - d. Click **Add**. Click on **Object Types** and verify that **Computers** are selected. Click **OK**.
 - e. Type in your `target_name` and click **CheckName**.
 - f. Select **Full Control**. Click **OK**.

4. Bring the source Exchange group online.



NOTE: You may need to create the source virtual network name in the Active Directory then force Active Directory replication before the Exchange virtual server network name resource will come online.

5. You will need to run the Exchange failover utility again to prepare the databases for use. In a command prompt window, execute the following command:

```
exchfailover -failback -onlypublicfolders -s source_Exchange_virtual_name  
-t target_Exchange_virtual_name
```

where `source_Exchange_virtual_name` is the name of the source Exchange virtual server and `target_Exchange_virtual_name` is the name of the target Exchange virtual server.

After the command completes, clients can connect through Outlook or Outlook Web Access to receive their e-mail.



NOTE: You can automate steps 1, 2, 4, and 5 by using the commands below. Step 3 can only be automated if you select the first option for modifying the security settings. The commands are case-sensitive and you will need to substitute the name of your source cluster, source virtual server, target virtual server, the resource name of the target Exchange IP address and disk(s), and the source Exchange group.

```
exchfailover.exe -setup -failback -s source_Exchange_virtual_name -t  
target_Exchange_virtual_name  
exchfailover -failback -nopublicfolders -s source_Exchange_virtual_name -t  
target_Exchange_virtual_name  
cluster /cluster:"target_cluster_name" res "target_Exchange_IP_resource_name"  
/online  
cluster /cluster:"target_cluster_name" res "target_Exchange_Disk_name" /online  
cluster /cluster:"source_cluster_name" group "Group_Name" /ONLINE  
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 25000  
exchfailover -failback -onlypublicfolders -s source_Exchange_virtual_name -t  
target_Exchange_virtual_name
```

Appendix 1: Updating Exchange components after the initial configuration

After you have completed the initial configuration and Storage Mirroring is mirroring and replicating, your Exchange components on the source may not be static. You may need to add a new information store to your Exchange configuration, or you may need to update to a new Exchange service pack. In these cases, you do not need to repeat the entire initial configuration. Use the appropriate instructions below, depending on the change you need to make.

Adding a new information store

1. On the source cluster, right-click on the Storage Mirroring Source Connection resource within the source Exchange group and select **Take Offline**.
2. On the target cluster, bring the unique target Exchange virtual server Network Name and the Exchange resources online.



NOTE: Do not bring the duplicate source IP online.

3. Create the information store on the target with the same name and location that will be created on the source.
4. Repeat step 3 for each new information store required.
5. Take the target Exchange group offline.



NOTE: If you selected a path that is outside of the existing replication set, you will need to modify the replication sets on the source cluster nodes to include the path(s) to the new data.

6. Bring the target Exchange disk(s) and target Exchange IP address resource online.



NOTE: Do not bring the duplicate source IP online.

7. On the source cluster, right-click on the Storage Mirroring Source Connection resource within the source Exchange group and select **Bring Online**.

When the difference mirror is complete, the target will be ready to stand in for the source with the new information store(s).

Applying an Exchange service pack or upgrade

1. On the source cluster, right-click on the Storage Mirroring Source Connection resource within the source Exchange group and select **Take Offline**.
2. Apply the Exchange service pack or upgrade.
3. On the target cluster, bring the target Exchange virtual server Network Name and the Exchange resources online.



NOTE: Do not bring the duplicate source IP online.

4. Apply the same Exchange service pack or upgrade, making sure that any settings applied are identical to the source cluster.
5. Take the Exchange group offline on the target cluster.
6. Bring the target Exchange IP address and target Exchange disk(s) online.



NOTE: Do not bring the duplicate source Exchange IP address online.

7. On the source cluster, right-click on the Storage Mirroring Source Connection resource within the source Exchange group and select **Bring Online**.

When the difference mirror is complete, the target will be ready to stand in for the source with the updated components.

Appendix 2: WAN failover

Because failover of Exchange across a WAN is dependent on DNS and Active Directory, Exchange availability after failover is dependent on Active Directory and DNS updates. Therefore, additional configuration requirements and specific WAN configuration steps must be completed before the Exchange server will be available to users.



NOTE: Due to the complexities of DNS and Active Directory in a WAN environment, this section of the document is intended for network administrators with experience in DNS, Active Directory, and Exchange. If you are unfamiliar with these features or are only familiar with the basics of these features, contact HP Technical Support.

WAN requirements

The following additional requirements must be addressed if your source and target clusters are on different subnets.

- Microsoft Exchange Server requires access to an Active Directory Domain Controller that is, at a minimum, configured as a Global Catalog Server.
- DNS Forward and Reverse lookup zones need to be properly configured per Microsoft standards.

In the event that the entire source cluster fails, you will need to perform some or all of the following steps before the clients can reconnect to the target cluster on a different subnet.

1. Update DNS. The types of DNS records that will need to be modified vary by implementation but may include A, MX, and CNAME records. There are three possible options for updating DNS after failover:
 - a. **Manual DNS updates**—You can update the DNS server manually by using the Windows Administrative Tools (Start, Programs, Administrative Tools, DNS).
 - b. **Automated/Scripted updates using DNSCMD**—The DNS Server Troubleshooting Tool utility (DNSCMD), which can be found in the Windows 200x support tools, can be used to add and delete DNS mappings. The commands are case-sensitive and can be executed from a command prompt or from within a batch file.

Several examples are shown below, where `ExchangeSourceName` is the name of the source Exchange virtual server and `ExchangeTargetName` is the name of the target Exchange virtual server:

```
dnscmd dns_server /RecordDelete mydomain.com @ MX 10
ExchangeSourceName.mydomain.com /f

dnscmd dns_server /RecordAdd mydomain.com @ MX 10
ExchangeTargetName.mydomain.com

dnscmd dns_server /RecordDelete mydomain.com WebMail CNAME
ExchangeSourceName.mydomain.com /f

dnscmd dns_server /RecordAdd mydomain.com WebMail CNAME
ExchangeTargetName.mydomain.com

dnscmd dns_server /RecordDelete mydomain.com Mail CNAME
ExchangeSourceName.mydomain.com /f

dnscmd dns_server /RecordAdd mydomain.com Mail CNAME
ExchangeTargetName.mydomain.com
```

```

dnsCMD dns_server /RecordDelete mydomain.com ExchangeSourceName A
xxx.xxx.xxx.xxx /f

dnsCMD dns_server /RecordDelete xxx.xxx.in-addr.arpa xxx.xxx PTR
ExchangeSourceName.mydomain.com /f

dnsCMD dns_server /RecordAdd mydomain.com ExchangeSourceName CNAME
ExchangeTargetName.mydomain.com

```

DNSCMD commands will only work if dynamic updates are enabled on the DNS zone. This is configured on the DNS zone Properties dialog box in the Windows Microsoft Management Console DNS snap-in. If Only Secure Updates is enabled (this option is available only on Active Directory-integrated zones), the DNSCMD utility must be used in the context of a user who is in the domain DnsAdmins group. This means the Storage Mirroring service logon account must be in the DnsAdmins group if the commands are in failover and fallback scripts. The Account option in the Storage Mirroring Monitor Settings does not apply to the failover and fallback scripts, so verify the Storage Mirroring service logon account is in the DnsAdmins group.

The Windows Dynamic DNS (DDNS) client does not initiate a registration reflecting the failed over name and IP address when failover occurs, and the ipconfig /registerdns command will not cause the failed over name and IP address to be registered. Accordingly, host records for the source will remain intact after failover and any required changes must be made on all DNS servers used by relevant clients. Changes to non-Windows DNS servers and Windows DNS servers with dynamic updates disabled must be implemented by some other means, but since DNS zone files are text-based, they can be manipulated with any scripting language that can open, parse, and write to a text file.

c. **Automated/Scripted updates using DNS WMI**—The DNS WMI Provider can be used to automate or script adding and deleting records to and from the DNS server. The steps vary based on the operating system.

- **Windows 2000**—For information on the DNS WMI Provider, visit msdn.microsoft.com and search for DNS WMI Provider. The following link can also be used: msdn.microsoft.com/library/en-us/dns/dns/installing_the_provider.asp

To download the DNS WMI Provider, use the following link: ftp.microsoft.com/reskit/win2000/dnsprov.zip

Once the DNS WMI Provider for Windows 2000 has been installed on the DNS Server, the included VBS scripts can be used to automate DNS record modifications.

- **Windows 2003**—The DNS WMI Provider is installed and configured by default on Windows 2003 DNS Servers, but the scripts necessary to modify DNS records are not pre-installed. Windows Server 2003 users will still need to download DNS WMI Provider for Windows 2000, which can be found at the following link: ftp.microsoft.com/reskit/win2000/dnsprov.zip

2. In a command prompt window, change to the Storage Mirroring directory, then execute the following command:

```
exchfailover -setup -failover -s ExchangeSourceName -t ExchangeTargetName
```

where ExchangeSourceName is the name of the source Exchange virtual server and ExchangeTargetName is the name of the target Exchange virtual server.

3. Once the command has finished executing, bring the Exchange resource group on the target cluster online.

4. If your source had the routing master, you will need to modify the security settings so that the routing master role will be updated. You have two options available for modifying the security settings for the routing master role:

- The first option grants the Exchange Failover utility the permission to perform the task for you. If you want to use this option, add the `-u username:password` switch as outlined in ["Exchange Failover Utility command syntax"](#) on page 33 to the `exchfailover` command in step 5. Specify the Exchange administrator account information.
- The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and fallback scripts. You will have to use ADSIEdit from the Windows Support Tools to make this change. See your Windows reference guide for more information.
 - a. Open ADSIEdit and go to `CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.
 - b. Right-click on the entry. Choose **Properties**.
 - c. Select the Security tab. Click **Advanced**.
 - d. Click **Add**. Click on **Object Types**.
 - e. Verify that **Computers** are selected. Click **OK**.
 - f. Type in your `target_name` and click **CheckName**.
 - g. Select **Full Control**. Click **OK**.



NOTE: By default, the Terminal Services server does not allow service interaction through remote desktop.

5. You will need to run the Exchange failover utility again to prepare the databases for use. Execute the following command:

```
exchfailover -failover -s ExchangeSourceName -t ExchangeTargetName
```

where `ExchangeSourceName` is the name of the source Exchange virtual server and `ExchangeTargetName` is the name of the target Exchange virtual server.



NOTE: After failover, you may need to use the Active Directory Sites and Services applet to force domain controller replication before clients can connect.

The Time To Live (TTL) of cached source mapping from DNS on network clients may affect the time that elapses from failover until clients can reconnect. Network clients will cache DNS mappings they have previously resolved for a length of time specified by the TTL value. The default is 15 minutes.

You may also need to manually close and reopen Outlook clients.

Appendix 3: WAN Failback

Because failback of Exchange across a WAN is dependent on DNS and Active Directory, Exchange availability after failback is dependent on Active Directory and DNS updates. Therefore, additional configuration requirements and specific WAN configuration steps must be completed before the Exchange server will be available to users.



NOTE: Due to the complexities of DNS and Active Directory in a WAN environment, this section of the document is intended for network administrators with experience in DNS, Active Directory, and Exchange. If you are unfamiliar with these features or are only familiar with the basics of these features, contact HP Technical Support.

WAN requirements

The following additional requirements must be addressed if your source and target clusters are on different subnets.

- Microsoft Exchange Server requires access to an Active Directory Domain Controller that is, at a minimum, configured as a Global Catalog Server.
- DNS Forward and Reverse lookup zones need to be properly configured per Microsoft standards.

Updating the source with the new data from the target

During the source downtime, users are updating data on the target cluster. When your source cluster is ready to come back online, the data is no longer current and must be updated with the new data from the target cluster.

1. Bring one or both of the source cluster nodes online, but do not allow the Exchange group to start.



NOTE: If necessary, you may have to disconnect one cluster node from the production network, bring it online, take the Exchange resource group offline, and then reconnect the node to the network.

2. Using the instructions in "[Creating the replication sets](#)" on page 12, create a replication set on the target cluster that includes all of the volumes contained in the target Exchange resource group.
3. Bring the Exchange physical disk resource(s) on the source cluster online.
4. Using the instructions in "[Completing the source configuration](#)" on page 15, create the Storage Mirroring Source Connection resource to the source cluster node IP address (not the source cluster virtual Exchange server IP address, which is offline). Modify the `ONLINE.DTCL` script and bring the resource online so that mirroring and replication to the source cluster can begin.
5. Monitor the mirroring process to ensure that it completes with no errors. The mirroring process is complete when the Mirror Status is Idle. Users may continue to access Exchange on the target cluster server. After the mirror completes, schedule downtime to convert operations back to the source cluster.

Taking the resources offline

 **NOTE:** At the scheduled downtime, you will be taking the Exchange resources offline. Clients will be unable to access mail services at this time.

1. Take the target Exchange virtual server Network Name resource offline. This should take every resource in the group offline except for the Storage Mirroring Source Connection, the Exchange IP address, and the disk resource(s).
2. Verify that all of the data in queue on the source cluster has been applied to the original source before continuing. You can verify that the source queue is empty by checking the Bytes in Target Disk Queue statistic in the Target section of DTStat or the Bytes in Queue statistic in the Storage Mirroring Target section of Performance Monitor. If these statistics are zero (0), the queue is empty and you can continue. If these statistics are not zero, there is still data in queue on the source and you must wait before continuing. For information on DTStat and Performance Monitor statistics, see the *HP OpenView Storage Mirroring user's guide*.
3. Once all of the data has been replicated, take the Storage Mirroring Source Connection resource offline on the target cluster and then delete it.

 **NOTE:** The Storage Mirroring Source Connection resource on the target is no longer needed after data has been restored to the original cluster.

Bringing the source Exchange group online

Complete the following steps to bring the source Exchange group online.

1. Like failover, DNS must be updated for failback. The types of DNS records that will need to be modified vary by implementation but may include A, MX, and CNAME records. There are three possible options for updating DNS after failover:
 - **Manual DNS updates**—You can update the DNS server manually by using the Windows Administrative Tools (Start, Programs, Administrative Tools, DNS).
 - **Automated/Scripted updates using DNSCMD**—The DNS Server Troubleshooting Tool utility (DNSCMD), which can be found in the Windows 200x support tools, can be used to add and delete DNS mappings. The commands are case-sensitive, and can be executed from within a batch file.

Several examples are shown below, where ExchangeSourceName is the name of the source Exchange virtual server and ExchangeTargetName is the name of the target Exchange virtual server:

```
dnscmd dns_server /RecordDelete mydomain.com ExchangeSourceName CNAME  
ExchangeTargetName.mydomain.com /f
```

```
dnscmd dns_server /RecordAdd mydomain.com ExchangeSourceName A  
xxx.xxx.xxx.xxx
```

```
dnscmd dns_server /RecordAdd xxx.xxx.in-addr.arpa xxx.xxx PTR  
ExchangeSourceName.mydomain.com
```

```
dnscmd dns_server /RecordDelete mydomain.com @ MX 10  
ExchangeTargetName.mydomain.com /f
```

```
dnscmd dns_server /RecordAdd mydomain.com @ MX 10  
ExchangeSourceName.mydomain.com
```

```

dnscmd dns_server /RecordDelete mydomain.com WebMail CNAME
ExchangeTargetName.mydomain.com /f

dnscmd dns_server /RecordAdd mydomain.com WebMail CNAME
ExchangeSourceName.mydomain.com

dnscmd dns_server /RecordDelete mydomain.com Mail CNAME
ExchangeTargetName.mydomain.com /f

dnscmd dns_server /RecordAdd mydomain.com Mail CNAME
ExchangeSourceName.mydomain.com

```

DNSCMD commands will only work if dynamic updates are enabled on the DNS zone. This is configured on the DNS zone Properties dialog box in the Windows Microsoft Management Console DNS snap-in. If Only Secure Updates is enabled (this option is available only on Active Directory-integrated zones), the DNSCMD utility must be used in the context of a user who is in the domain DnsAdmins group. This means the Storage Mirroring service logon account must be in the DnsAdmins group if the commands are in failover and failback scripts. The Account option in the Storage Mirroring Monitor Settings does not apply to the failover and failback scripts, so verify the Storage Mirroring service logon account is in the DnsAdmins group.

The Windows Dynamic DNS (DDNS) client does not initiate a registration reflecting the failed over name and IP address when failback occurs, and the ipconfig /registerdns command will not cause the failed over name and IP address to be registered. Accordingly, host records for the source will remain intact after failback and any required changes must be made on all DNS servers used by relevant clients.

Changes to non-Windows DNS servers and Windows DNS servers with dynamic updates disabled must be implemented by some other means, but since DNS zone files are text-based, they can be manipulated with any scripting language that can open, parse, and write to a text file.

- **Automated/Scripted updates using DNS WMI**—The DNS WMI Provider can be used to automate or script adding and deleting records to and from the DNS server. The steps vary based on the operating system.
 - **Windows 2000**—For information on the DNS WMI Provider, visit msdn.microsoft.com and search for DNS WMI Provider. The following link can also be used: msdn.microsoft.com/library/en-us/dns/dns/installing_the_provider.asp

To download the DNS WMI Provider, use the following link:
ftp.microsoft.com/reskit/win2000/dnsprov.zip

Once the DNS WMI Provider for Windows 2000 has been installed on the DNS Server, the included VBS scripts can be used to automate DNS record modifications.

- **Windows 2003**—The DNS WMI Provider is installed and configured by default on Windows 2003 DNS Servers, but the scripts necessary to modify DNS records are not pre-installed. Windows Server 2003 users will still need to download DNS WMI Provider for Windows 2000, which can be found at the following link:
ftp.microsoft.com/reskit/win2000/dnsprov.zip

2. In a command prompt window, change to the Storage Mirroring directory, then execute the following commands:

```

exchfailover -setup -failback -s ExchangeSourceName -t ExchangeTargetName
exchfailover -failback -nopublicfolders -s ExchangeSourceName -t
ExchangeTargetName

```

where ExchangeSourceName is the name of the source Exchange virtual server and ExchangeTargetName is the name of the target Exchange virtual server.

3. If you moved the routing master role to the target, you will need to modify the security settings so that the routing master role will be updated back to the source. You have two options available for modifying the security settings for the routing master role:
 - The first option grants the Exchange Failover utility the permission to perform the task for you. If you want to use this option, add the `-u username:password` switch as outlined in ["Exchange Failover Utility command syntax"](#) on page 33 to the `exchfailover` command in step 5. Specify the Exchange administrator account information.
 - The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and fallback scripts. You will have to use ADSIEdit from the Windows Support Tools to make this change. See your Windows reference guide for more information.
 - a. Open ADSIEdit and go to `CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.
 - b. Right-click on the entry. Choose **Properties**.
 - c. Select the Security tab. Click **Advanced**.
 - d. Click **Add**. Click on **Object Types** and verify that **Computers** are selected. Click **OK**.
 - e. Type in your `target_name` and click **CheckName**.
 - f. Select **Full Control**. Click **OK**.
4. Once the commands in step 2 have finished executing, bring the source cluster Exchange resource group online.
5. You will need to run the Exchange failover utility again to prepare the databases for use. In a command prompt window, execute the following command:
`exchfailover -failback -onlypublicfolders -s ExchangeSourceName -t ExchangeTargetName`

where `ExchangeSourceName` is the name of the source Exchange virtual server and `ExchangeTargetName` is the name of the target Exchange virtual server.

After the command completes, clients can connect to the Exchange server and access mail services.



NOTE: After failback, you may need to use the Active Directory Sites and Services applet to force domain controller replication before clients can connect. You may also need to manually close and reopen Outlook 2000 clients.

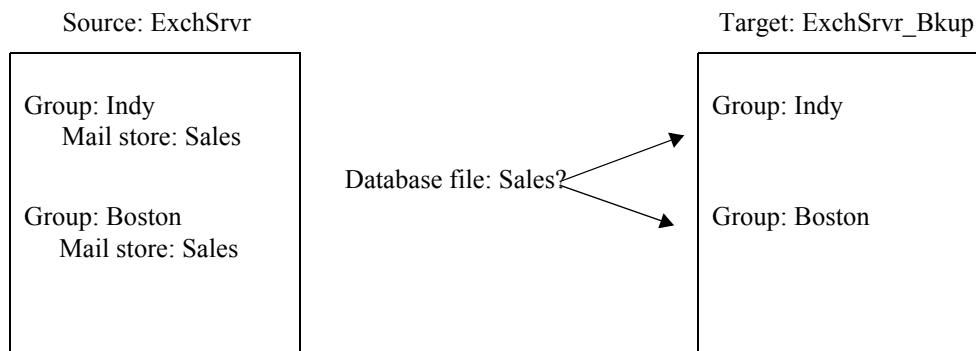
The Time To Live (TTL) of cached source mapping from DNS on network clients may affect the time that elapses from failback until clients can reconnect. Network clients will cache DNS mappings they have previously resolved for a length of time specified by the TTL value. The default is 15 minutes.

You may also need to manually close and reopen Outlook clients.

Appendix 4: Configuring additional Exchange Failover Utility options

In order for a mail store (and its users) to be failed over (or failed back), a mail store on the source must be paired to a mail store on the target. In order to be a valid pair, the database filename (excluding path information) of these two stores must match. The Exchange Failover utility uses two methods to make these mail store pairs. The simplest (default) method requires that the database filenames be unique and that each filename only occurs once on the source and once on the target.

For example, a server called ExchSrvr contains two mail groups, Indy and Boston. Each group contains a mail store called Sales. In its simplest form, the Exchange Failover utility would not know which group to associate the Sales mail store with since it is based on the database file name.

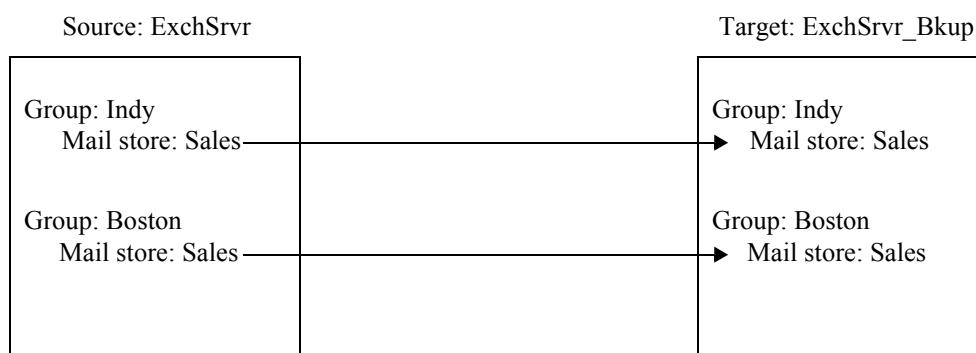


To resolve this issue, you can direct the groups and mail stores to meet your environment needs. The `-r` option in the Exchange Failover utility is a pairing rule. It allows you to specify how the groups and mail stores on the source will be paired on the target.

By itself, the `-r` option will create a one-to-one mapping from the source to the target. For example, the command

```
exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r
```

would automatically create a one-to-one mapping on the target.



You can be more specific with the `-r` option and direct the source groups to specific group names on the target. For example, the command

```
exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r Indy:Indy_Bkup -r Boston:Boston_Bkup
```

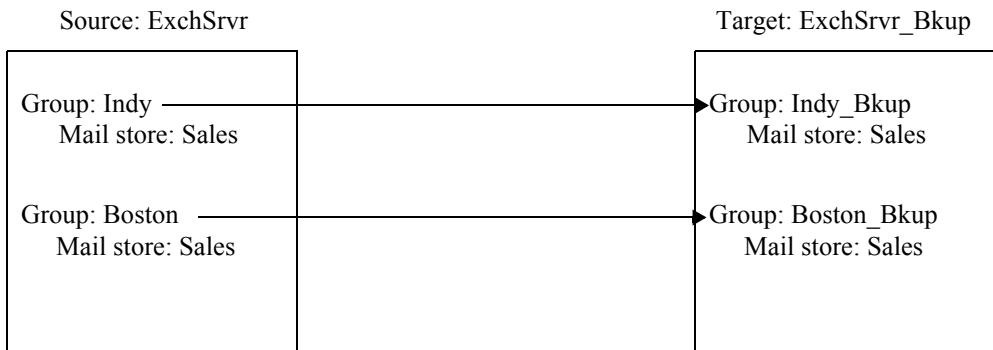
will pair the mail stores from the source Indy group in the group `Indy_Bkup` on the target. The mail stores from the source Boston group will be paired in the group `Boston_Bkup` on the target. The following diagram illustrates this pairing.



If needed, you can be the most specific with the `-r` option by specifying both the group and mail store names. For example, if you need to direct the group and mail store names on the target, the command

```
exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r Indy,  
Sales:Indy_Bkup, Sales -r Boston, Sales:Boston_Bkup, Sales
```

will pair the mail store `Sales` in the `Indy_Bkup` group from the `Sales` mail store from the `Indy` group on the source. It will also pair the mail store `Sales` in the `Boston_Bkup` group from the `Sales` mail store from the `Boston` group on the source.



There are several other options available in the Exchange Failover utility. These options and the full command syntax are included in ["Exchange Failover Utility command syntax"](#) on page 33.

Exchange Failover Utility command syntax

Command	EXCHFAILOVER
Description	Used in script files to failover Exchange data
Syntax	<pre>EXCHFAILOVER -FAILOVER -FAILBACK -s <source> -t <target> [-l <log_filename>] [-norus] [-nospn] [-nopublicfolders] [-onlypublicfolders] [-o <options_filename>] [-r [<source_group>[,<source_mail_store>] [:[:<target_group>] [,<target_mail_store>]]] [-SETUP] [-test] [-u <username>:<password>] [-? [?]]</pre>
Options	<ul style="list-style-type: none">• FAILOVER—The Exchange data will be moved from the source to the target during failover• FAILBACK—The Exchange data will be moved from the target to the source during failback• s <i>source</i>—The name of the original source server• t <i>target</i>—The name of the original target server• l <i>log_filename</i>—The name of the optional log file name. By default, the log file is <code>ExchFailover.log</code> and is stored in the directory containing the <code>exchfailover.exe</code> file. If this name is changed, the <code>DTInfo</code> utility will not be able to locate this file which could impede assistance through Technical Support.• norus—Do not change the Recipient Update Service• nospn—Do not change the Service Principle Name• nopublicfolders—Do not move the public folders• onlypublicfolders—Only move the public folders• o <i>options_filename</i>—Allows you to pass in a file containing the options for the Exchange Failover utility• r—By itself, this option creates a one-to-one mapping of the groups and mail stores from the source to the target• r <i>source_group:target_group</i>—The <i>r</i> option with the group names will direct the source group name specified to the target group name specified• r <i>source_group, source_mail_store:target_group, source_mail_store</i>—The <i>r</i> option with all of the <i>r</i> options will direct the source group name and mail store specified to the target group name and mail store specified• SETUP—Allows you to set the overwrite database on restore flag without completing user moves or RUS and folder updates. If the <code>-setup</code> switch is not supplied, the utility still sets the overwrite database on restore flag, but the other work is performed also.• test—Test mode that does not change the Exchange configuration• u <i>username:password</i>—A user with Active Directory permissions• ?—Displays the syntax of the Exchange Failover utility• ??—Displays the syntax of the Exchange Failover utility along with brief descriptions of each option

Examples	<ul style="list-style-type: none"> • exchfailover -failover -s Indy -t ExchSrvr_Bkup • exchfailover -failover -s Indy -t ExchSrvr_Bkup -r • exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales • exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales, Inside:Indy_Sales, Inside -r Sales, Outside:Indy_Sales, Outside • exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales -norus -u administrator:password • exchfailover -failover -s Indy -t ExchSrvr_Bkup -o options_file.txt
Notes	<ul style="list-style-type: none"> • When using the -failback option, the source-related options pertain to your original source or what will become the new source, if the original source had to be replaced. The target-related options pertain to the target that is currently standing in for the source. • The password specified with the -u option is the only case-sensitive option in this command.

Appendix 5: Security requirements

When performing failover operations, you should be logged in under the LocalSystem account, which is the same as the Microsoft Exchange System Attendant service. This configuration should provide sufficient permissions for most operations that occur during failover, including DNS updates, SPN updates, changes to the Active Directory schema, and updating mailbox properties for each user.



NOTE: Depending on your environment, a lower level of permissions may be applied.

SPN updates

Failover

During failover, the source server's Active Directory SPNs will be moved to the target server's Active Directory object. In order to accomplish this, the `Write servicePrincipalName` permission on the source's computer account in Active Directory must be assigned to the account that will modify the SPNs, which can be either of the following:

- The target's Storage Mirroring service logon account. If the target's Storage Mirroring service is configured to log on as the System account, the target's Active Directory computer account should be assigned the permissions.
- The account specified in the failover monitor configuration

Write or Full Control permissions (which are assigned to Domain Administrators by default) can also be used to assign `Write servicePrincipalName` permissions.

Use the following procedure to assign the `Write servicePrincipalName` permission to a user or group.

1. Open ADSIEDIT and go to `CN=Server_Name, CN=Computers, DC=Domain_name, DC=com`.
2. Right-click on the entry, then choose **Properties**.
3. Select the Security tab, then click **Advanced**.
4. Click **Add**. Click on **Object Types** and verify that **Computers** is selected. Click **OK**.
5. Type in your `target_name` and click **CheckName**.
6. Select **Full Control**, then click **OK**.

Failback

During failback, the `Write servicePrincipalName` permission on the target's computer account in Active Directory must be assigned back to the account that will modify the SPNs on the source.

To update the permissions on the source, follow the SPN Failover procedure, except assign Full Control to your `source_name` instead.

Routing master

Failover

If your source server is the routing master, you will need to modify the security settings so that the routing master role can be moved to the target. There are two options available for modifying the security settings for the routing master role:

- Use the `-u` parameter and specify an ID that has sufficient authority to perform the operations.
- Change specific Active Directory attributes to allow the update to be performed by the scripts.

You must use ADSIEDit (from the Windows Support Tools) to assign the correct permissions to allow for the updating of the Routing Master.

1. Open ADSIEDit and go to `CN=Routing Groups, CN=Computers, DC=Domain_name, DC=com`.
2. Right-click on the entry, then choose **Properties**.
3. Select the Security tab, then click **Advanced**.
4. Click **Add**. Click on **Object Types** and verify that **Computers** is selected. Click **OK**.
5. Type in your `target_name` and click **CheckName**.
6. Select **Full Control**, then click **OK**.

Failback

If your source server was the routing master, you will need to modify the security settings so that the routing master role can be returned.

To update the permissions on the source, follow the Routing Groups Failover procedure, except assign Full Control to your `source_name` instead.

Recipient Update Service

Failover

The target machine must have the ability to modify the Recipient Update Service information. This involves allowing specific permissions to the Exchange Organization.

1. Open ADSIEdit and go to CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com.
2. Right-click on the entry, then choose **Properties**.
3. Select the Security tab, then click **Advanced**.
4. Click **Add**. Click on **Object Types** and verify that **Computers** is selected. Click **OK**.
5. Type in your `target_name` and click **CheckName**.
6. Select **Full Control**, and click **OK**.

Fallback

During failback, the ability to modify the Recipient Update Service information must be assigned back to the source.

To update the permissions on the source, follow the Recipient Update Service Failover procedure, except assign Full Control to your `source_name` instead.